

09/446511

416 ~~Recd PCT/PTO~~ 27 DEC 1999

APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. PM 265420
(M#)

Invention: TRANSACTION METHOD WITH A MOBILE DEVICE

Inventor (s): RITTER, Rudolf
BOUQUET, Hanspeter
HEUTSCHI, Walter

Pillsbury Madison & Sutro LLP
Intellectual Property Group
1100 New York Avenue, NW
Ninth Floor
Washington, DC 20005-3918
Attorneys
Telephone: (202) 861-3000

This is a:

- Provisional Application
- Regular Utility Application
- Continuing Application
- PCT National Phase Application
- Design Application
- Reissue Application
- Plant Application
- Substitute Specification
Sub. Spec Filed
in App. No. / _____

SPECIFICATION

Transaction Method with a Mobile Device

This invention relates to a method and a system for transmission of orders in a telecommunications network. The invention relates in particular, but not 5 exclusively, to the transmission of orders in a mobile radio network.

According to the state of the art thus far, transactions between a customer (or client, C) and a terminal [point-of-transaction (POT)], for example a point-of-sale (POS), are often carried out with an electronic payment card. Debit and credit cards are used, for example, at cash points in shops, at gas stations, etc.

10 The card usually comprises memory means, for example a magnetic strip and/or a chip, in which the identification of the customer, *inter alia*, is stored. To carry out a transaction with the owner or operator of a terminal, for example to pay for an article in a shop, the customer has to push his card into a suitable card reader in the terminal. The terminal then reads the identification of the customer in the 15 card, establishes and displays the amount to be paid, checks, if necessary, the solvency of the customer, and asks the customer to confirm the transaction with a confirmation key on the terminal. If the customer is solvent and has given his confirmation, the customer identification, the amount to be paid, and possibly also a terminal identification are transmitted to a finance server connected with the 20 terminal through a telecommunications network, which server is administered by a financial institution. The account of the customer with this financial institution is accordingly debited immediately or later.

Disadvantageous with this method is the necessity of having to push the card of the customer into a foreign device. The customers normally do not have 25 their cards at hand, but rather, for example, in their wallets; a very fast transaction is thus not possible. Also sometimes the aperture for insertion of the card into the reading device of the terminal is not easily accessible; this is especially the case when the terminal is a ticket machine for parking garages or a payment machine, which is supposed to be operated by the automobile driver without getting out of 30 the car. Moreover fraudulent acts or unauthorized readings of the memory areas of the card can be carried out in the terminal.

Even if certain chipcards nowadays contain a microprocessor, these debit cards and credit cards are essentially passive elements which store data that is memorized and used essentially by the electronics of the terminal. The customer, on the other hand, usually has no opportunity of direct access to the data without 5 going to a counter or to an automatic machine of the respective financial institution which issues the card. It is therefore difficult for the customer to check the transactions carried out with the card and to keep a record of them.

These cards contain a customer identification, however, which only allows the customers to be identified at the issuing financial institution. Thus a card can 10 normally only be used for a financial transaction if the customer and the terminal operator are associated with the same financial institution. On the other hand, use of the card for other types of transactions – for example for non-financial transactions for which reliable identification of the customer/ card holder is necessary, however – is not foreseen. Owning a large number of cards for every 15 type of financial and non-financial transactions is therefore unavoidable for the customer, for example several debit cards or credit cards, which are administered by various financial institutions or chains of stores, or subscription cards or access cards for protected zones. These cards are usually protected by various pin codes, which the customer must laboriously memorize.

20 In the case of theft or a fraudulent act using the card, the card must be disabled. The disabling cannot take place, however, until the card has been inserted into a corresponding device. The common credit cards can continue to be used, however, in manually operated apparatuses; a secure blocking of the card is thus not possible.

25 Besides debit cards and credit cards, so-called e-cash cards (value cards) are also known, which enable monetary amounts to be stored electronically, which are then accepted at various terminals as means of payment. To provide these cards again with monetary amounts, the customer must go to the counter or machine of a financial institution, which is not always possible.

30 One object of the present invention is to propose a method or system which allows these problems to be avoided.

A further object of the present invention is to propose a transaction method which is suitable both for financial as well as for non-financial transactions, and which is simpler and more reliable than the common transaction methods.

These objects are attained according to the present invention through the 5 elements of the characterizing part of the independent claims. Further preferred embodiments follow moreover from the dependent claims and the description.

In particular these objects are achieved through a transaction method between a customer and a terminal (for example a point of sale, POS) connected to a telecommunications network, which method comprises the features of the 10 independent claims.

The present invention will be more comprehensible with the aid of the description given as an example and illustrated through the attached figures:

Figure 1 shows a block diagram, which shows the information flow in a first embodiment of the system according to the invention, the customer being 15 equipped with a mobile radio telephone, preferably a GSM or UMTS mobile device, which can receive and transmit special short messages.

Figure 2 shows a block diagram which shows the information flow in a second embodiment of the system according to the invention, the customer being equipped with a mobile radio telephone, preferably a GSM or UMTS mobile 20 device, which can receive and transmit special short messages, and the terminal being an Internet or Intranet-capable device.

Sub A Figure 3 shows a flow chart of a payment transaction method according to the invention.

Figure 4 shows a flow chart of a reloading transaction method of a SIM 25 card, according to the invention.

The method represented in Figures 3 and 4 can be carried out with any system variant, shown, for example, in Figures 1 and 2. The first and the second variants both require a mobile radio telephone with a SIM card and an additional infrared or inductive interface, which will be described more closely later.

Figure 1 shows the information flow in a first embodiment of the invention. The customer is equipped with a mobile radio telephone which comprises a mobile device, for example a GSM or UMTS mobile device 1 and an identification module 10, e.g. a SIM card. The number 11 designates an operating unit, e.g. a keyboard. The customer is identified in the mobile radio network 6 with an identification module 10. The SIM card has a conventional microcontroller 100, which is embedded in the plastic supporting base of the card and which is responsible for the GSM functions of the card – such as are described, for example, in the article “SIM cards” by T. Grigorova and I. Leung, which appeared 10 in the *Telecommunication Journal of Australia*, vol. 43, No. 2, 1993, on pages 33 to 38 – and for new functions which are loaded onto the SIM card at a later point in time. The SIM card can preferably be a JAVA-capable card, i.e. a card with a processor which can carry out the instructions in the JAVA programming language (or in another object-oriented language). SIM cards according to the Opencard 15 concept of IBM can also be used. The SIM card has in addition contact means, not shown, via which the card communicates with the mobile device 1 in which it is inserted.

The SIM card has moreover a second processor 101 (CCI, Contactfree Chipcard Interface), which is responsible for the contactless connection with the 20 POT device 2. The second processor carries out, *inter alia*, the TTP (Trusted *<sic. Trusted>* Third Party) functions, described further below, to receive and transmit encoded and signed messages. A logical interface 102 connects the two processors 101 and 102. Optionally a single processor could replace these two processors 101, 102.

25 The contactless interface with the terminal 2 can have, for example, at least one inductance (not shown) integrated into the SIM card and connected to the second processor 101, with which data are transmitted inductively in both directions via a radio path. In a variant, an inductive coil can also be integrated into the housing of the mobile device. In still a further variant, the contactless 30 interface comprises an infrared transmitter-receiver on the housing of the mobile device. In a further variant, the contactless interface is integrated into an

extension module, which can be removably connected to the mobile device. The contactless communication between the two devices is preferably encrypted, for example with a DEA, DES, TDES, RSA or EEC security algorithm.

Alv

- 5 The contactless communication is based preferably on a named standard, for example on the IrDA (Infrared Data Association) protocol. Error checking and error correcting means are preferably used for this communication. Terminal identification means are preferably used in addition to establish reliably a connection with just one particular terminal, should a plurality of terminals, e.g. several mobile devices and/or several terminals, be combined in a room.
- 10 With an inductive signal transmission from the terminal to the chipcard, a phase modulation method is preferably used, whereas in the reverse direction, preferably the amplitude of the signals is modulated.

The SIM card preferably contains a special field IDUI (International Debit User Identification), with which the customer is identified by the terminal operator and/or by a financial institution. The IDUI identification is preferably stored in a first protected memory area of one of the two processors 101, 102. The IDUI contains at least an identification of the network operator, a user number which identifies him from other customers with the same network operator, a user class indication which defines which services he may use, and optionally in addition a country identification. The IDUI contains moreover security data, *inter alia* a transaction counter T_z , a loading token LT_c , and a time-out field TO , which indicates the validation time. The function of these different data will be explained later.

The SIM card contains in addition a second, protected memory area in which electronic monetary units (monetary amounts) can be stored.

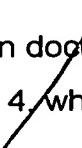
The symbolically represented terminal 2 is likewise provided with a contactless transceiver 20, for example with an inductive coil or with an infrared transmitter-receiver. Thanks to this interface, the mobile system 1, 10 can communicate in a contactless way with the device 2 in both directions.

The terminal 2 can be, for example, a point-of-sale (POS) in a shop specially equipped with a radio interface 20, and is identified with a special field POSID (Point of Sale Identification). The POSID depends upon the application; in the case of a shop cash point, it contains an identification of the network operator, 5 an area identification (sub-region in a country), a POS number which identifies it from other POS with the same network operator, a POS class indication which defines which services it may use or offer, the date, the time, the currency used (SDR, Euros or dollars), and optionally, in addition, a country indication.

The terminal 2 is preferably provided with data input means, not shown, for 10 example with a keyboard, and with data display means, not shown, for example with a screen.

The IDUI identification is transmitted to the terminal via the contactless interface 10/101, and is linked in the terminal with the POSID and with the captured transaction amount A, so that an electronic transaction document is 15 produced, which is signed and encrypted with a TTP (Trusted Third Party) or PTP (Point-To-Point) method.

The transaction document is then transmitted via a modem, not shown, and through the communications network 5, for example through a public switched telephone network to the clearing unit 3, likewise connected to the network 5. 20 This unit receives the electronic documents from various terminals 2, independently of the country or communications region, and independently of the country or financial institution of the customer. In the clearing unit 3 these transaction documents are ordered according to financial institution, possibly also according to operator, and are delivered to the service center 4, 4', 4'' of the 25 respective financial institution. Clearing units in themselves are already known in the GSM technology, and are used, for example, for collecting and for further distributing connection costs. The clearing unit can contain, for example, a data base which indicates with which financial institution the customer, previously identified with his IDUI, is affiliated.

Sub A  The electronic transaction documents handled by the clearing unit 3 are passed on to the service center 4, which has preferably a finance server. In the

120
100
80
60
40
20
0
100
120
140
160
180
200
220
240
260
280
300
320
340
360
380
400
420
440
460
480
500
520
540
560
580
600
620
640
660
680
700
720
740
760
780
800
820
840
860
880
900
920
940
960
980
1000
1020
1040
1060
1080
1100
1120
1140
1160
1180
1200
1220
1240
1260
1280
1300
1320
1340
1360
1380
1400
1420
1440
1460
1480
1500
1520
1540
1560
1580
1600
1620
1640
1660
1680
1700
1720
1740
1760
1780
1800
1820
1840
1860
1880
1900
1920
1940
1960
1980
2000
2020
2040
2060
2080
2100
2120
2140
2160
2180
2200
2220
2240
2260
2280
2300
2320
2340
2360
2380
2400
2420
2440
2460
2480
2500
2520
2540
2560
2580
2600
2620
2640
2660
2680
2700
2720
2740
2760
2780
2800
2820
2840
2860
2880
2900
2920
2940
2960
2980
3000
3020
3040
3060
3080
3100
3120
3140
3160
3180
3200
3220
3240
3260
3280
3300
3320
3340
3360
3380
3400
3420
3440
3460
3480
3500
3520
3540
3560
3580
3600
3620
3640
3660
3680
3700
3720
3740
3760
3780
3800
3820
3840
3860
3880
3900
3920
3940
3960
3980
4000
4020
4040
4060
4080
4100
4120
4140
4160
4180
4200
4220
4240
4260
4280
4300
4320
4340
4360
4380
4400
4420
4440
4460
4480
4500
4520
4540
4560
4580
4600
4620
4640
4660
4680
4700
4720
4740
4760
4780
4800
4820
4840
4860
4880
4900
4920
4940
4960
4980
5000
5020
5040
5060
5080
5100
5120
5140
5160
5180
5200
5220
5240
5260
5280
5300
5320
5340
5360
5380
5400
5420
5440
5460
5480
5500
5520
5540
5560
5580
5600
5620
5640
5660
5680
5700
5720
5740
5760
5780
5800
5820
5840
5860
5880
5900
5920
5940
5960
5980
6000
6020
6040
6060
6080
6100
6120
6140
6160
6180
6200
6220
6240
6260
6280
6300
6320
6340
6360
6380
6400
6420
6440
6460
6480
6500
6520
6540
6560
6580
6600
6620
6640
6660
6680
6700
6720
6740
6760
6780
6800
6820
6840
6860
6880
6900
6920
6940
6960
6980
7000
7020
7040
7060
7080
7100
7120
7140
7160
7180
7200
7220
7240
7260
7280
7300
7320
7340
7360
7380
7400
7420
7440
7460
7480
7500
7520
7540
7560
7580
7600
7620
7640
7660
7680
7700
7720
7740
7760
7780
7800
7820
7840
7860
7880
7900
7920
7940
7960
7980
8000
8020
8040
8060
8080
8100
8120
8140
8160
8180
8200
8220
8240
8260
8280
8300
8320
8340
8360
8380
8400
8420
8440
8460
8480
8500
8520
8540
8560
8580
8600
8620
8640
8660
8680
8700
8720
8740
8760
8780
8800
8820
8840
8860
8880
8900
8920
8940
8960
8980
9000
9020
9040
9060
9080
9100
9120
9140
9160
9180
9200
9220
9240
9260
9280
9300
9320
9340
9360
9380
9400
9420
9440
9460
9480
9500
9520
9540
9560
9580
9600
9620
9640
9660
9680
9700
9720
9740
9760
9780
9800
9820
9840
9860
9880
9900
9920
9940
9960
9980
10000
10020
10040
10060
10080
10100
10120
10140
10160
10180
10200
10220
10240
10260
10280
10300
10320
10340
10360
10380
10400
10420
10440
10460
10480
10500
10520
10540
10560
10580
10600
10620
10640
10660
10680
10700
10720
10740
10760
10780
10800
10820
10840
10860
10880
10900
10920
10940
10960
10980
11000
11020
11040
11060
11080
11100
11120
11140
11160
11180
11200
11220
11240
11260
11280
11300
11320
11340
11360
11380
11400
11420
11440
11460
11480
11500
11520
11540
11560
11580
11600
11620
11640
11660
11680
11700
11720
11740
11760
11780
11800
11820
11840
11860
11880
11900
11920
11940
11960
11980
12000
12020
12040
12060
12080
12100
12120
12140
12160
12180
12200
12220
12240
12260
12280
12300
12320
12340
12360
12380
12400
12420
12440
12460
12480
12500
12520
12540
12560
12580
12600
12620
12640
12660
12680
12700
12720
12740
12760
12780
12800
12820
12840
12860
12880
12900
12920
12940
12960
12980
13000
13020
13040
13060
13080
13100
13120
13140
13160
13180
13200
13220
13240
13260
13280
13300
13320
13340
13360
13380
13400
13420
13440
13460
13480
13500
13520
13540
13560
13580
13600
13620
13640
13660
13680
13700
13720
13740
13760
13780
13800
13820
13840
13860
13880
13900
13920
13940
13960
13980
14000
14020
14040
14060
14080
14100
14120
14140
14160
14180
14200
14220
14240
14260
14280
14300
14320
14340
14360
14380
14400
14420
14440
14460
14480
14500
14520
14540
14560
14580
14600
14620
14640
14660
14680
14700
14720
14740
14760
14780
14800
14820
14840
14860
14880
14900
14920
14940
14960
14980
15000
15020
15040
15060
15080
15100
15120
15140
15160
15180
15200
15220
15240
15260
15280
15300
15320
15340
15360
15380
15400
15420
15440
15460
15480
15500
15520
15540
15560
15580
15600
15620
15640
15660
15680
15700
15720
15740
15760
15780
15800
15820
15840
15860
15880
15900
15920
15940
15960
15980
16000
16020
16040
16060
16080
16100
16120
16140
16160
16180
16200
16220
16240
16260
16280
16300
16320
16340
16360
16380
16400
16420
16440
16460
16480
16500
16520
16540
16560
16580
16600
16620
16640
16660
16680
16700
16720
16740
16760
16780
16800
16820
16840
16860
16880
16900
16920
16940
16960
16980
17000
17020
17040
17060
17080
17100
17120
17140
17160
17180
17200
17220
17240
17260
17280
17300
17320
17340
17360
17380
17400
17420
17440
17460
17480
17500
17520
17540
17560
17580
17600
17620
17640
17660
17680
17700
17720
17740
17760
17780
17800
17820
17840
17860
17880
17900
17920
17940
17960
17980
18000
18020
18040
18060
18080
18100
18120
18140
18160
18180
18200
18220
18240
18260
18280
18300
18320
18340
18360
18380
18400
18420
18440
18460
18480
18500
18520
18540
18560
18580
18600
18620
18640
18660
18680
18700
18720
18740
18760
18780
18800
18820
18840
18860
18880
18900
18920
18940
18960
18980
19000
19020
19040
19060
19080
19100
19120
19140
19160
19180
19200
19220
19240
19260
19280
19300
19320
19340
19360
19380
19400
19420
19440
19460
19480
19500
19520
19540
19560
19580
19600
19620
19640
19660
19680
19700
19720
19740
19760
19780
19800
19820
19840
19860
19880
19900
19920
19940
19960
19980
20000
20020
20040
20060
20080
20100
20120
20140
20160
20180
20200
20220
20240
20260
20280
20300
20320
20340
20360
20380
20400
20420
20440
20460
20480
20500
20520
20540
20560
20580
20600
20620
20640
20660
20680
20700
20720
20740
20760
20780
20800
20820
20840
20860
20880
20900
20920
20940
20960
20980
21000
21020
21040
21060
21080
21100
21120
21140
21160
21180
21200
21220
21240
21260
21280
21300
21320
21340
21360
21380
21400
21420
21440
21460
21480
21500
21520
21540
21560
21580
21600
21620
21640
21660
21680
21700
21720
21740
21760
21780
21800
21820
21840
21860
21880
21900
21920
21940
21960
21980
22000
22020
22040
22060
22080
22100
22120
22140
22160
22180
22200
22220
22240
22260
22280
22300
22320
22340
22360
22380
22400
22420
22440
22460
22480
22500
22520
22540
22560
22580
22600
22620
22640
22660
22680
22700
22720
22740
22760
22780
22800
22820
22840
22860
22880
22900
22920
22940
22960
22980
23000
23020
23040
23060
23080
23100
23120
23140
23160
23180
23200
23220
23240
23260
23280
23300
23320
23340
23360
23380
23400
23420
23440
23460
23480
23500
23520
23540
23560
23580
23600
23620
23640
23660
23680
23700
23720
23740
23760
23780
23800
23820
23840
23860
23880
23900
23920
23940
23960
23980
24000
24020
24040
24060
24080
24100
24120
24140
24160
24180
24200
24220
24240
24260
24280
24300
24320
24340
24360
24380
24400
24420
24440
24460
24480
24500
24520
24540
24560
24580
24600
24620
24640
24660
24680
24700
24720
24740
24760
24780
24800
24820
24840
24860
24880
24900
24920
24940
24960
24980
25000
25020
25040
25060
25080
25100
25120
25140
25160
25180
25200
25220
25240
25260
25280
25300
25320
25340
25360
25380
25400
25420
25440
25460
25480
25500
25520
25540
25560
25580
25600
25620
25640
25660
25680
25700
25720
25740
25760
25780
25800
25820
25840
25860
25880
25900
25920
25940
25960
25980
26000
26020
26040
26060
26080
26100
26120
26140
26160
26180
26200
26220
26240
26260
26280
26300
26320
26340
26360
26380
26400
26420
26440
26460
26480
26500
26520
26540
26560
26580
26600
26620
26640
26660
26680
26700
26720
26740
26760
26780
26800
26820
26840
26860
26880
26900
26920
26940
26960
26980
27000
27020
27040
27060
27080
27100
27120
27140
27160
27180
27200
27220
27240
27260
27280
27300
27320
27340
27360
27380
27400
27420
27440
27460
27480
27500
27520
27540
27560
27580
27600
27620
27640
27660
27680
27700
27720
27740
27760
27780
27800
27820
27840
27860
27880
27900
27920
27940
27960
27980
28000
28020
28040
28060
28080
28100
28120
28140
28160
28180
28200
28220
28240
28260
28280
28300
28320
28340
28360
28380
28400
28420
28440
28460
28480
28500
28520
28540
28560
28580
28600
28620
28640
28660
28680
28700
28720
28740
28760
28780
28800
28820
28840
28860
28880
28900
28920
28940
28960
28980
29000
29020
29040
29060
29080
29100
29120
29140
29160
29180
29200
29220
29240
29260
29280
29300
29320
29340
29360
29380
29400
29420
29440
29460
29480
29500
29520
29540
29560
29580
29600
29620
29640
29660
29680
29700
29720
29740
29760
29780
29800
29820
29840
29860
29880
29900
29920
29940
29960
29980
30000
30020
30040
30060
30080
30100
30120
30140
30160
30180
30200
30220
30240
30260
30280
30300
30320
30340
30360
30380
30400
30420
30440
30460
30480
30500
30520
30540
30560
30580
30600
30620
30640
30660
30680
30700
30720
30740
30760
30780
30800
30820
30840
30860
30880
30900
30920
30940
30960
30980
31000
31020
31040
31060
31080
31100
31120
31140
31160
31180
31200
31220
31240
31260
31280
31300
31320
31340
31360
31380
31400
31420
31440
31460
31480
31500
31520
31540
31560
31580
31600
31620
31640
31660
31680
31700
31720
31740
31760
31780
31800
31820
31840
31860
31880
31900
31920
31940
31960
31980
32000
32020
32040
32060
32080
32100
32120
32140
32160
32180
32200
32220
32240
32260
32280
32300
32320
32340
32360
32380
32400
32420
32440
32460
32480
32500
32520
32540
32560
32580
32600
32620
32640
32660
32680
32700
32720
32740
32760
32780
32800
32820
32840
32860
32880
32900
32920
32940
32960
32980
33000
33020
33040
33060
33080
33100
33120
33140
33160
33180
33200
33220
33240
33260
33280
33300
33320
33340
33360
33380
33400
33420
33440
33460
33480
33500
33520
33540
33560
33580
33600
33620
33640
33660
33680
33700
33720
33740
33760
33780
33800
33820
33840
33860
33880
33900
33920
33

with a suitable menu on the screen of the computer 2. The customer can control this computer with his mobile device. For example, he can control the position of the cursor in a menu of products or information offered for sale by actuating the cursor movement keys on the keyboard 11 of his mobile telephone. The cursor movement instructions are transmitted via the contactless interface 101, 20 to the computer 2'. The user actuates a confirmation key, for example the key # on his keyboard, in order to confirm the selected menu option, for example to order a product.

The customer identification stored in the mobile device 1, 10 is linked, in an electronic transaction document, with the POSID and with the transaction amount corresponding to selected menu option, is TTP or PTP encrypted and signed. The transaction document contains preferably a customer identification IDUI taken out of the SIM card 10, a supplier identification corresponding to the dialed menu option, and a product identification corresponding to the dialed menu option, preferably in Flexmart format as proposed in the patent application PCT/CH96/00464. This document is established through a Flexmart module 21. The Flexmart module is preferably a software application carried out by the computer 2'.

Analogously to the first embodiment, the electronic transaction document is then transmitted to the respective finance server 4, 4' or 4" through the clearing unit 3 and is processed there.

A payment transaction method will now be more closely described with the aid of Figure 3. This method can be applied to any embodiments of the invention according to Figures 1 and 2. This procedure is generally valid, however, and not limited to GSM and UMTS methods.

The first column in Figure 3 shows the method steps which involve mainly the mobile radio telephone 1 of the customer; the second describes the method steps which are executed by the terminal 2; the third relates to the operations of the service center 4, and the fourth/the effects on the various accounts at the financial institution . It must be noted, however, that many method steps can be carried out either with the mobile radio telephone 1, for example as a process

inside the SIM card 10, or in the terminal 2. For example, the data input can take place either with the terminal or with the mobile radio telephone 1, if this contains a keyboard, such as, for example, a GSM mobile device.

This method sets the prerequisite in step 200 that the identification card 10 of the customer comprises a protected memory area in which electronic monetary units are stored. Value cards in themselves are known; we shall explain more closely later, with reference to Figure 4, how the monetary amount can be reloaded. In addition, the patent application EP 96810570.0 describes a method of reloading SIM cards with a monetary amount.

The mobile system 1, respectively 10, is switched into operation readiness in step 201, for example with the switching on of the mobile device. In step 202 the terminal 2 is likewise activated. Then in step 203 the terminal 2 calls the next, unspecific customer in a broadcast method (card paging).

When the connection between the terminal 2 and the mobile radio telephone 1, 10 has been established, the mobile radio telephone presents in step 204 its identification IDUI (International Debit User Identification) to the terminal and the confirmation that it is solvent. The IDUI is filed in a first protected area of the card. Whether the solvency suffices cannot yet be decided at this moment.

The terminal 2 contains a black list, preferably periodically updated by the finance server 4, on customers to be blocked. The IDUI transmitted by the customer is compared with the black list (step 205) (authorization data). If the IDUI presented by the customer is found in the black list (step 206), a blocking flag is set in step 207. If there is no correspondence, the transaction amount A can be entered on the keyboard of the terminal 2. In a variant, the transaction amount A can also be entered with the input means 11 of the mobile device 1. The terminal 2, or in a variant the SIM card 10, then links this amount to the identification of the terminal 2 and of the IDUI, and transmits this debit document to the customer. Preferably a reference currency is moreover included, for example SDR, Euros or dollars.

Since the communication is signed, it can be checked in step 210 whether the debit document correlates to the IDUI. If not, the refusal reason is displayed on the terminal 2 (step 223). Otherwise a check for a blocking flag is made in step 211. If it is set (212), a check-up with the finance server 4 follows (step 248).

5 If it is not set, an area check-up follows (step 213). SIM cards can thereby be blocked depending on the area of use. If the area check-up is negative, a check-up with the finance server 4 (step 248) follows; otherwise a time-out check-up is made (step 215). It is checked whether the validation time, during which transactions can be carried out without check-up, has already expired. If the

10 validation time has expired (step 216), a check-up with the finance server takes place (step 248); otherwise the customer is asked in step 217 to enter manually his user password on the mobile device 1. If the entered password is correct (step 218), the amount A is converted, if necessary, into the standard currency (for example SDR) (step 219). An international application of the concept is

15 thereby made possible. Otherwise, the refusal, with indication of reason, is displayed on the terminal 2 in step 223.

The mobile radio telephone 1/10 then checks in step 220 whether the transaction amount A to be debited is covered by the monetary amount loaded in the second memory area (solvency check). If this is not the case, this refusal reason is displayed on the screen of the terminal (step 223).

20 *Sig 4* When all these checks have been made, the transaction is counted in step 222 with a transaction counter T_z which is incremented. This meter corresponds to the number of transactions carried out with the card 10. In step 224, the transaction amount A, the terminal identification POSID and the user identification 25 IDUI are then linked in a transaction document, which is moreover certified and optionally encrypted, and possibly also compressed. The ECC method (Elliptic Curve Cryptosystem) can be used, for example, for the certification. A suitable certification and encryption method will be more closely explained later as an example.

30 The charged transaction amount A is then debited against the stored monetary amount account in step 225, and the transaction document is filed in a

stack on the identification module 10 in step 226. This card stack at the customer can be called up by the finance server 4 as needed for the purpose of detailed checking. The customer himself can preferably display on his mobile device 1 the transaction documents stored in the stack.

*Sub
C5*

After step 224 the transaction document is presented to the terminal 2 for billing, and the customer signature is checked by the terminal (step 227). Optionally, in step 228, a paper receipt is printed out on the terminal for the customer.

In step 229, then in the terminal 2, the debit document is possibly linked

10 with additional data, and the transaction document is electronically signed by the terminal 2, optionally compressed and encoded. The electronic transaction document prepared in this way is then optionally filed in a stack in the terminal 2 in step 230. The stack contains transaction documents of various customers. The transaction documents are then transmitted during step 231 individually or

15 grouped to the clearing unit 3. The transmission can either take place immediately after the transaction, or a plurality of transaction documents from the stack can be transmitted at periodic time intervals (for example every hour or everyday). A batch process can also be used to transmit all transaction documents, for example at night.

20 The clearing unit 3 receives individual or grouped transaction documents from a plurality of terminals 2 in the same geographic zone (step 234). A plurality of geographically distributed clearing units can be provided. In step 235, the clearing unit 3 allocates the transaction documents received from the various terminals to the respective financial institutions or services providers, and passes

25 these transaction documents on accordingly.

If the transaction documents are encoded, they first have to be decrypted by the clearing unit in order to be allocated to a finance server 4, 4', 4'', and then encoded again by the clearing unit in order to pass them on. In a preferred variant, however, the data elements in the fields IDUI and possibly POSID of the

30 transaction document, which are needed for the clearing, are not encoded by the terminal 2. Achieved thereby can be a secured, end-to-end encrypted

transmission of the transaction documents between the terminals and the finance servers 4, 4', 4".

Sig 6

The responsible finance server receives the transaction documents, in step 236, and the TTP server 40 decompresses and decrypts them (if necessary), and

5 checks the authenticity of the signatures from the terminal 2 and from the identification module 10. In step 237, it is checked whether the POSID and/or the IDUI is to be found in a revocation list. If the test is positive (238), because neither the terminal identification nor the customer identification IDUI are located on the revocation list, a test of the loading token LT follows in step 239. The

10 loading token LT gives the number of reloadings of the card 10. This loading token is updated in the finance server (LT_s) and in the identification module (LT_c) after each reloading process, as explained later. A copy of the loading token LT_c is transmitted in the transaction document in the field IDUI. The loading token LT_c , reported by the mobile radio telephone 1, 10 must be equal to the loading

15 token LT_s stored in the finance server 4. If reloading documents are still on the way between the finance server 4 and the mobile system 1, 10, LT_c can also be temporarily smaller than LT_s . The finance server 4 therefore checks whether

$LT_c \leq LT_s$.

Sig 7

If this condition is not verified in step 240, probably an unauthorized reloading process was carried out, and the method goes on to step 241.

Distinguished here is whether the falsification has been carried out by the terminal or by the customer. If the customer is responsible, he is entered on a black list in step 242. A customer blocking document is preferably generated and sent to the mobile radio telephone 1, 10 of the customer in order to set the blocking flag and

25 to disable this system, as well as to all terminals or at least all terminals in a predefined geographic area in order to enter this customer in the black list of that terminal. If, on the other hand, the problem was caused by the terminal, this terminal is entered in a terminal black list in step 243.

If the loading token check is passed in step 240, the transaction amount A

30 in the transaction document can be debited against a customer control account at the financial institution in step 244. In step 245, the transaction amount A is

accordingly credited to an account 420, 420' or 420" of the terminal operator at a financial institution. Processing charges can also be debited against the account 420 and/or against a customer account by a financial institution and/or by the terminal operator or by the network operator.

5 Then in step 246 the finance server 4 enters this transaction in the transaction counter. Then a process follows in step 247 to update the values of the loading token LT_c and of the transaction counter Tz in the mobile radio telephone.

Sub C7
10 We refer back to the process in the mobile radio telephone 1, 10. As already explained, this device arrives at step 248 if a security problem has been noted in step 212, 214 or 216. In this case, a complete check-up with the finance server takes place, preferably via the mobile radio network 6. The check-up comprises, for example, a test and a renewal of the authentication certificate as well as a check of all executed parameters, for example the loading token LT , the 15 transaction counter Tz , the black list, etc. If the result of the check-up is negative (step 249), the blocking flag is set so that the mobile system 1 is disabled, or at least the respective use in the SIM card 10 (step 253). If, on the other hand, this examination shows that most probably no falsification was attempted, the validation time is reset in step 250. With the validation time, an identification 20 module can be disabled, for example, if it has not been used for a predefined period, for example one year. This indication must therefore be reset after each use. The blocking flag is then cancelled in step 251, and, if necessary, a new area is set in step 252.

It is important to note that the debiting process can take place with different 25 currencies, for example on the basis of the SDR (Special Drawing Rights) common in the telecommunications sphere or with another reference currency (for example Euros or dollars). The maximal amount on the card is defined according to the client class. A default value in SDR is possible as minimal. Each terminal 2 stores the SDR value (e.g. currency-specific) relevant for it, which is 30 communicated to it by the server in the registration process. Depending upon

exchange rate fluctuations, the terminals are automatically supplied with updated exchange rates by the finance server.

Sieg 08 A method of reloading the mobile system 1, 10 with a monetary amount will now be described more closely with reference to Figure 4. This method can likewise be applied to any embodiments of the invention according to Figures 1 or 2.

A reloading process takes place in this example with the mobile radio telephone 1, 10 of the client and the terminal 2 together. It would also be possible, however, to carry out <reloading of> the monetary amount on the identification module 10 with a transaction which only affects the mobile radio telephone 1, 10 and the service center 4. This solution would have the advantage that the customer would not have to go to a terminal; certain security checks cannot be executed in this case, however. This variant is therefore preferably used only for transmitting smaller monetary amounts or when additional security mechanisms are provided. A direct reloading process by the finance server 4 could also be used, however. Depending upon the client class, or depending upon need, the document card stack at the customer can be called up by the finance server for the purpose of detailed checking. After the reloading process, the stack can be deleted by the finance server.

The first column in Figure 4 shows the method steps which principally involve the mobile radio telephone 1, 10; the second describes the method steps which are carried out by the terminal 2; the third relates to the operations of the service center 4, and the fourth the effects on the various accounts at the financial institution. It must be noted, however, that many method steps can be carried out either with the mobile radio telephone 1, 10, for example inside the SIM card 10, or with the terminal 10. For example, the steps of the method that relate to the data input can be carried out either on the terminal or on the mobile device, if the mobile device contains an operating unit. The communication between the two parts is preferably encrypted, for example with a DEA, DES, TDES, RSA or EEC security algorithm.

In step 300, the mobile radio telephone 1, 10 is first operatively cleared for the reloading process; the terminal 2, for its part, is also activated in step 301.

The terminal 2 then calls the next, unspecified mobile system 1, 10 in a broadcast method in step 302 (card paging).

Sub a

When the connection is made between the terminal 2 and the mobile radio telephone 1, 10, the customer presents to the terminal, in step 303, his identification IDUI (International Debit User Identification) and the type of the process to be started, here a reloading.

The terminal 2 contains a black list on mobile systems to be blocked (revocation list), preferably updated periodically by the finance server 4. The IDUI transmitted by the customer is compared with the black list (step 304). If the IDUI presented by the customer is found in the black list (step 305), a blocking flag is set in step 306. Afterwards, or if no correspondence is found, whether the request correlates with the IDUI is checked in step 307. If not, the refusal reason is displayed on the terminal 2 (step 315). Otherwise the blocking flag is checked in step 308. If it is set, the mobile radio telephone 1, 10, or at least the respective application in the identification card 10, is disabled (step 331). If it is not set, the customer is asked in step 310 to enter his password manually in the mobile device 1. If the entered password is not correct (step 311), the blocking flag is likewise set, and the refusal reason is displayed on the terminal 2 (step 315); otherwise the method is clear for reloading, and the customer is asked in step 312 to enter a reloading amount A. In the variant shown, the reloading amount can be entered on the terminal 2; this amount is linked in step 313 with the POSID and the IDUI, signed and transmitted to the card 10. The amount A could, however, also be captured at the mobile device 1; in this case no terminal is involved and the POSID is therefore not needed.

In step 314 it is checked whether the IDUI in the data received from the terminal 2 coincides with the own IDUI. If not, the refusal reason is displayed on the terminal 2 (step 315); otherwise the desired reloading amount entered on the terminal is displayed on the screen of the mobile device 1. Then in step 316, the POSID (optional), the IDUI, the already mentioned number of payment transactions Tz, the number of reloading processes (LTc, loading token client) stored on the card, and the remaining amount on the card DRA (Debit Rest

Card

Amount) are linked, signed, encrypted and then optionally compressed. A reloading document is thereby produced. Optionally, the document stack on the card can also be transmitted, for example depending upon the client class, with the issuing of the card, or as needed during use with solvency problems. The

5 POSID is only integrated into the reloading document if the customer has a mobile device without suitable input means. The reloading document is then transmitted to the finance server 4, 4', respectively 4'', through the network 6, where the TTP server 40 receives, if necessary decrypts and decompresses this document in step 317, and checks the signature of the customer and, if applicable, of the

10 terminal.

With the aid of the table 318, which stores the number and token relating to the processes between the customer and the finance server, the following checks are made in step 319:

Check of amounts: The sum ΣA of all amounts loaded on the identification module 10, including the start sum, must be equal to or smaller than the sum of all control charges ΣK_B and the remaining amount $D_R A$ on the identification module. The sum can be smaller because the documents which are still between the mobile radio system 1, 10, the clearing unit 3 and the finance server 4, 4', 4'', cannot yet be captured at this moment.

Step 319

Check of loading token: The number of loading, or respectively reloading, transactions are counted in the mobile radio telephone, for example in the SIM card using a token $L_T c$ and in the finance server 4 using another token $L_T s$. These two token *<sic. tokens>* must be equal.

Check of transaction counter: For each payment transaction, the transaction counter T_z in the mobile radio telephone 1, 10 is incremented; the T_z is also carried over in each reloading document. The transaction counter T_{zs} stored at the finance server, which is incremented by the documents transferred by the customer, must be equal to, or possibly smaller than, the transaction counter T_z in the mobile radio telephone 1, 10.

If one of these three conditions is not fulfilled (step 320), the blocking flag is set in step 321, and the reloading process is refused in step 325. Otherwise, in step 322, the account balance 41 of the customer is checked. If it does not suffice for the reloading, the refusal is likewise processed in step 325.

Sub 5.1

If the account (or the account limit) of the customer at the financial institution 4 suffices for the amount to be reloaded (step 322, 323), this amount is withdrawn from a customer account of the financial institution (324), including any fees. At the same time the requested reloading amount is booked on the control account 41. A reloading document is then produced in step 326 from the POSID, the IDUI, the amount A, the new loading token LTn, and a predefined time-out increment TOi. This reloading document is signed in step 327, optionally encrypted and compressed, and transmitted to the mobile system 1, 10 of the customer. This system checks during step 328 whether the signature in the document comes from the finance server, and verifies during step 329 whether the blocking flag is set. If it is set (step 330), the mobile radio telephone 1, or at least the respective application, is disabled in step 331. Otherwise it is further checked whether the finance server has requested a refusal (step 332) leading to interruption of the process with display of the reason for refusal (step 334).

If all tests have been successfully passed, the card account is booked in step 335 with the requested reloading amount. The old loading token LTC is then replaced by the new loading token LTn (step 336), transmitted by the finance server. The transaction counter Tz on the card is set back in the next step 337, and the time-out TOi is reset in step 338. In addition, a new area is set in step 340 if, in step 339, it is determined that the POSID is contained in the reloading document.

The reloading amount is then displayed as confirmation, either on the screen of the mobile device or on the terminal (step 341). Finally, the total balance of the account on the card is also displayed (step 342).

In the example described with the aid of Figures 3 and 4, the "real" bank account of the customer at the financial institution is already debited during reloading of the card. Other payment variants, for example with credit cards or by

drawing up an invoice, are also possible of course within the framework of this invention. In a variant, the system can also function as a credit system: in this case the bank account of the customer is first debited when the finance server 7 receives a transaction document. The monetary amount stored in the second 5 memory area of the card serves in this case only as the expenditure limit.

The securing of data transmissions through cryptography is carried out differently in two different segments. Between the customer and the terminal, the communication through the air interface is secured, for example, through an algorithm, such as DES, TDES, RSA or EEC. Between the customer and the 10 finance server, on the other hand, the TTP (Trusted Third Party) method, or optionally a PTP (Point-To-Point) method is used. The necessary elements are integrated on the identification element 10 and in the TTP server 40. The transaction documents are preferably encrypted with a symmetrical algorithm, whereby the symmetrical algorithm uses a session key encrypted with an 15 asymmetrical algorithm. In addition, the transmitted transaction documents are preferably certified.

PRINTED FROM FEDERAL REGISTER